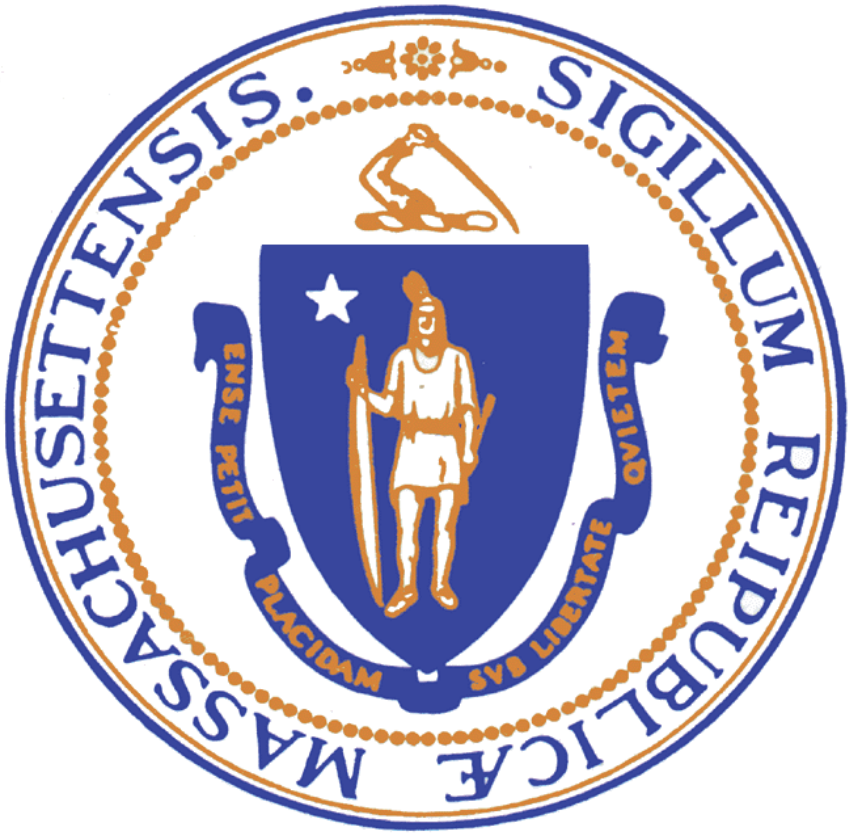
Commonwealth of Massachusetts

State Homeland Security Strategy



Mitt Romney, Governor
Kerry Healey, Lt. Governor
Edward A. Flynn, Secretary of Public Safety

As approved by the Office of Domestic Preparendess
February 6, 2004

The Commonwealth of Massachusetts
Executive Office of Public Safety

One Ashburton Place, Room 2113
Boston, Massachusetts 02108
Tel: (617) 727-6300
Fax: (617) 727-5356
TTY Tel: (617) 927-0238
www.mass.gov/eops

Mitt Romney
Governor

Kerry Healey
Lieutenant Governor

Edward A. Flynn
Secretary

February 27, 2004

I am pleased to present the State Homeland Security Strategy (SHSS) for the Commonwealth of Massachusetts. This strategy was submitted to the Department of Homeland Security, Office of Domestic Preparedness in accordance with requirements as defined in the FY 2004 Homeland Security Grant Program (HSGP) guidelines. Through this program, the Department of Homeland Security provides planning, equipment, training, exercise, and management funding to emergency prevention, preparedness and response personnel in all 50 states. HSGP program guidelines required that each state submit for approval a SHSS that defines the strategic vision, goals and objectives that will guide how the state government (departments, agencies and authorities) will work in partnership with federal, regional, local and private sector entities to enhance statewide capabilities to detect, prevent, respond to and manage the consequences of acts of terrorism and other critical incidents. Funding obtained through this program must be utilized to implement the goals and objectives defined in the SHSS. On February 17, 2004, the Commonwealth received formal notification that its submission had been approved by the Department of Homeland Security.

This statewide homeland security strategy represents a compilation of input, ideas and recommendations received from federal, state, local, and private sector officials through a series of meetings and other planning activities held throughout the state during the year 2003. The strategy takes into account the results of a statewide inventory of homeland security activities conducted by the Executive Office of Public Safety during the spring of 2003 and the Massachusetts homeland security assessment completed by local entities during the later half of 2003 (this assessment included a risk, capabilities, and needs assessment). This strategy also incorporates results of a comprehensive threat, vulnerability and risk assessment completed by the Massachusetts State Police Criminal Intelligence Section on January 31, 2004. These components will now be used to assist local public safety officials in the development and implementation of regional homeland security plans that are consistent with the overall state strategy.

This strategy is a critical step toward enhancing the Commonwealth's ability to work with its federal, regional and local partners to protect the people who live in, work in and visit the Commonwealth from future acts of terrorism or other catastrophic events. It will ensure that homeland security efforts statewide will proceed in a coordinated, consistent manner, adhering to the same central strategy. I am proud of the work that went into this strategy, from all levels of state and local government.

I look forward to working with you in the coming months as we work together to implement this statewide strategy.

Sincerely,

Edward A. Flynn
Secretary of Public Safety

TABLE OF CONTENTS

INTRODUCTION

This document serves as the State Homeland Security Strategy (SHSS) for the Commonwealth of Massachusetts. It provides the strategic vision that will guide how the state government (departments, agencies and authorities), will work in partnership with federal, regional, local and private sector entities, to enhance statewide capabilities to detect, prevent, respond to and manage the consequences of acts of terrorism and other critical incidents.

This statewide strategic plan represents a compilation of input, ideas and recommendations received from federal, state, local, and private sector officials through a series of meetings and other planning activities held throughout the state during the year (2003). The strategic plan takes into account the results of a statewide inventory of homeland security activities conducted by the Executive Office of Public Safety during the spring of 2003 and the Massachusetts homeland security assessment completed by local entities during the later half of 2003 (this assessment included a comprehensive risk, capabilities, and needs assessment). This strategy also incorporates results of a comprehensive threat, vulnerability and risk assessment completed by the Massachusetts State Police Criminal Intelligence Section.

The Commonwealth of Massachusetts will utilize resources provided by the Department of Homeland Security to support a multi-disciplinary approach to homeland security. This approach will emphasize detection, prevention, and information driven response and consequence management planning. The Commonwealth will take steps to ensure that all homeland security related funding received from the Department of Homeland Security and other federal entities is utilized in a coordinated manner. The Commonwealth will use these funds to:

- Offset the cost of planning activities;
- Acquire equipment and technology;
- Develop training programs;
- Plan and conduct training exercises; and
- Any other purposes expressly authorized by the federal government

It will be a top priority for the Commonwealth to enhance its ability to collect, analyze and distribute critical terrorism related intelligence and other relevant information. The collection, analysis and distribution of this information will serve as the foundation for a multi-disciplinary, proactive, risk mitigation approach to homeland security. Up-to-date, threat, vulnerability and risk information will be used to guide all operational planning and training activities.

The Massachusetts Vision for Homeland Security

Statewide Adaptation of the "All-Hazards" Approach

The Commonwealth will adopt an "all hazards" approach to homeland security. These efforts will be guided by the understanding that efforts to detect, prevent, respond to, and manage the consequences of acts of terrorism and other critical incidents are a twenty-four hour a day, seven days a week responsibility and part of the operational culture of state and local government. Building upon the solid foundation provided by — and in partnership with — the Joint Terrorism Task Force and the United States Attorney's Anti-Terrorism Advisory Council, the Commonwealth will take aggressive steps to enhance the capabilities of state, local and private sector entities so that they can better support the continuum of efforts necessary to ensure that homeland security related activities are proactive, information driven and multi-disciplined and ultimately guided by five fundamental principles:

- Terrorists often commit "traditional" crimes to support their extremist agenda and frequently they often collaborate with individuals involved in "traditional" criminal activity;

- Homeland security efforts are more effective when they involve the daily collaboration between core disciplines including, but not limited to, law enforcement, fire services, emergency medical, emergency management, health care, social service, transportation, environmental protection, public utilities, agriculture, general services, natural resources, and corrections;

- The same proactive, information driven and multi-disciplinary methods used to effectively mitigate crime, disorder, public health, social service and other emerging problems serve as the foundation for homeland security related efforts;

- Efforts to protect residents, workers and visitors of the Commonwealth from future acts of terrorism need not be done at the expense of effective day-to-day service. Nor must the Commonwealth invest millions of dollars in technology and equipment that will only be used in the event of a terrorist attack. In fact, the very information technology, communication systems, and business processes that support effective service delivery each and every day provide the foundation for effective efforts to detect, prevent and respond to terrorism and other critical incidents; and

- The Commonwealth will not compromise its commitment to uphold civil liberties and to sustain and dramatically strengthen the Commonwealth's proactive, positive partnership with the increasingly diverse communities throughout the Commonwealth.

The Governor has designated the Secretary of the Executive Office of Public Safety (EOPS) as the state's Homeland Security Advisor.[1] Accordingly, EOPS will coordinate statewide efforts to detect, prevent, respond to and manage the consequences of a terrorist attack or other critical incident. The Executive Office of Public Safety will establish a working partnership with various disciplines of federal, state and

local government (law enforcement, fire, emergency medical, emergency management, transportation, health care, general services, environmental, etc…) and private sector entities in carrying out this function. The activities of state departments, agencies and independent authorities will be coordinated through a multi-disciplinary Homeland Security Executive Committee comprised of executives from various state cabinet departments.[2] The Homeland Security Executive Committee will work in partnership with federal entities and local entities that will be organized into with multi-disciplinary regional consortiums modeled in part on the metropolitan Boston Urban Area Security Initiative.

(Footnotes)

[1] *As defined by the United States Department of Homeland Security.*

[2] *Commonwealth's Department of Fire Services, Executive Office of Public Safety, Department of Public Health, Massachusetts State Police, Criminal History Systems Board, MBTA Transit Police Department, MassPort, Executive Office of Transportation and Construction, The National Guard, Massachusetts Aeronautics Commission, and the Massachusetts Emergency Management Agency. Additionally, the metropolitan Boston Urban Area Security Initiative has appointed a representative to serve on the Homeland Security Executive Committee.*

Goals and Objectives

Goal #1 – The Commonwealth will enhance its ability to assess risk and prevent future terrorist attacks or critical incidents.

The Department of Homeland Security defines prevention as "actions to avoid an incident, to intervene to stop an incident from occurring, or to mitigate an incident's effect. It involves actions to protect lives and property and to defend against attacks. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; investigations to determine the full nature and source of the threat; public health surveillance and testing processes; immunizations, isolation or quarantine; and law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity."[3]

The loss of life and financial repercussions that would result from a successful terrorist incident requires that the Commonwealth of Massachusetts take aggressive steps to prevent such an attack from occurring. As a part of its SHSS, the Commonwealth will enhance its capacity to detect and prevent attacks (and other critical incidents). To achieve its goals, the Commonwealth in conjunction with federal, regional and local partners will take steps to:

- Produce up-to-date threat, vulnerability and risk information;
- Work with public and private sector entities to develop and implement problem-solving techniques that effectively address emerging threat conditions and environmental factors that may increase the vulnerability of relevant location(s) by enhancing physical security or taking other actions designed to minimize risks to assets;
- Support performance-based risk minimization and homeland security-related problem-solving efforts;
- Through an expansion of the state's Citizen Corp efforts, mobilize and train local community members and private sector officials to work with state and local personnel to identify unusual circumstances, while respecting privacy and ensuring that heightened awareness does not spark unnecessary alarm; and
- Ensure the effective flow of information among federal, state, local and private sector entities.
- Through a partnership of public health officials, ensure ongoing monitoring of emergency health events.

[3] *Department of Homeland Security, National Response Plan, page 8.*

A key component of the Commonwealth's homeland security efforts will be the state's ability to work with local, regional, federal and private sector partners to identify the parts of the state's critical infrastructure that are most at risk and taking steps to 'mitigate those risks."[4]

It is both unproductive and fiscally irresponsible for the Commonwealth to adopt a statewide homeland security strategy that fails to use specific risk related data to guide funding, planning and training efforts. It should be noted, however, that to be meaningful from an operational and training perspective, assessing threat, vulnerability and risk means more than the one-time collection of law enforcement information. It must include developing the capacity to "blend" – on an ongoing basis — public safety information with other important information (public health, transportation, financial services, social service, etc.) in order to:

- Rapidly identify emerging threats;
- Support multi-disciplinary, proactive and community focused problem solving activities;
- Support predictive analysis capabilities; and
- Improve the delivery of emergency and non-emergency services.

The Executive Office of Public Safety will work closely with other state entities and its federal, regional, local and private sector partners to establish an ongoing threat, vulnerability and risk identification and mitigation process. This process will guide all homeland security related operational planning, equipment acquisitions and training activities. The process will include completing a baseline threat, vulnerability and risk assessment that will be updated on an ongoing basis. Threat, vulnerability and risk -related information will regularly be shared with relevant federal, state, local and private sector officials and these officials will work in partnership to develop and execute performance based risk mitigation strategies. As part of this process, the Commonwealth will take steps to:

- Establish a prioritized list of potential targets and potential methodologies of attack;
- Share target lists with key officials;
- Identify conditions, environmental or otherwise, that may facilitate the ability of a terrorist to successfully carry out an attack;
- Establish a process for identifying and tracking key "indicators" of evolving/emerging terrorist-related activity;
- Monitor these indicators as part of the daily management of service related information;
- Disseminate important information to key individuals/entities and support the development and implementation of risk mitigation efforts; and

[4] *As the Commonwealth expands its ability to collect and analyze threat-related information, it must also take steps to ensure that this information is protected from inappropriate disclosure including the use of existing provisions established in state law.*

- Develop and track defined performance metrics that will allow for performance-based management of risk mitigation efforts.

Goal #2 – The Commonwealth will improve its ability to collect, analyze, disseminate and manage key information.

The operational and organizational "hub" of the Commonwealth's homeland security efforts will be a 24/7 information fusion center maintained by the Massachusetts State Police Criminal Intelligence Section (Fusion Center). The Fusion Center will collect, on an ongoing basis, an assortment of information (including but not limited to threat and vulnerability, terrorism, public safety, law enforcement, public health, social service, public works, transportation, etc.) from federal, state, county and local sources.[5] Highly trained personnel will process, evaluate and analyze relevant information that will then be used by policy makers and state, local and private sector personnel in support of:

- Risk mitigation efforts;
- Tactical and operational planning;
- The development of training exercises;
- The development of programmatic performance metrics; and
- The allocation of funding.

In order to maximize the capabilities of the Fusion Center and reduce the potential for duplication of effort, the Commonwealth will work closely with the Joint Terrorism Task Force, United States Attorney's Office and other key state, regional, and local entities to:

- Follow provisions of 28 Code of Federal Regulations (CFR) pertaining to Criminal Intelligence Systems operating policies (Chapter 1, Part 23 in particular);
- Establish a 24/7 information center that will serve as an "all source, multi-disciplinary intelligence fusion center;"
- Conduct an information needs analysis as a component of the intelligence/information fusion center;
- Ensure that intelligence/information requirements are formulated in a clear and concise manner;
- Ensure that the information gathering and sharing system includes all "owners" of key assets/critical infrastructures;

[5] *For example, it will be a priority for the Commonwealth to establish linkages between the Fusion Center and the various Operational Control Centers operated by Massachusetts Highway Authority, MassPort, MBTA, Massachusetts Turnpike Authority and Boston Transportation Department.*

- Establish a workable and reasonable "tier-line" approach for the sharing of information with other agencies, jurisdictions and the private sector;

- Ensure appropriate multi-disciplinary representation in the Fusion Center including establishing linkages with federal, state, regional, local and private sectors entities;

- Establish the information system using plans and processes that reasonably assure that all terrorist-related activity is reported to the Fusion Center;

- Identify "intelligence and information requirements" with sufficient specificity to alert observers to watch for certain things and train them to forward the information to the fusion center;

- Establish coordination points with related agencies to share information, strategies and tactics;

- Establish a clear path of information from multi-disciplinary observers to the fusion center; and

- Conduct education/training periodically to test observation of suspicious events and behaviors.

Goal #3 – The Commonwealth will improve preparedness by enhancing regional coordination.

The Department of Homeland Security defines preparedness as the "activities necessary to build and sustain performance across other domains. In one sense, preparedness is part of the life cycle of a specific incident in that it includes the range of deliberate, time-sensitive tasks that need to occur in the transition from prevention to response. Preparedness can also be characterized as a continuous process or cycle. The mission of preparedness is to develop meaningful answers to the question, 'are we prepared to be aware of, to prevent, to respond to, and to recover from terrorist attacks, major disasters, and other emergencies?' Preparedness involves efforts at all levels of government and within the private sector to identify risks or threats, to determine vulnerabilities, to inventory resources available to address those vulnerabilities, and to identify requirements or shortfalls, resulting in preparedness plans to remedy shortfalls over time. Preparedness plans include program initiatives for planning, training, equipping, exercising and evaluating capabilities to ensure sustainable performance in order to prevent, prepare for and respond to incidents."[6]

Unfortunately, aggressive awareness and prevention efforts cannot provide a 100% guarantee that all terrorist attacks will be prevented. Therefore, it must be a top priority for the Commonwealth to be prepared to mitigate the wide range of potential activities by terrorists (and others) including, threats, hoaxes, small scale attacks designed to disrupt service and attacks designed to cause mass casualties.

To support effective planning and preparation, local entities within defined geographical areas will be encouraged to form regional, multi-disciplinary (public safety, legal, health, social services, private sector, transportation, public works, etc…) consortiums (such as that established as part of the Boston area Urban Area Security Initiative [UASI]) to support the development of:

- Risk mitigation strategies;

- Response and consequence management plans;

[6] *Department of Homeland Security, National Response Plan, page 8.*

- Training programs and exercises; and

- Equipment acquisitions.

Being prepared requires constant planning, training, equipping and exercising. It requires consistent evaluation of sustainable performance in order to prevent, prepare for and respond to incidents. It also requires diligence in providing funding to support these emergency preparedness efforts. Once established, these regional consortiums will be expected (and supported) to:

- Identify all agencies conducting anti-terrorism and critical incident response planning activities;

- Identify and establish relationships between all responder agencies/groups within that region;

- Update emergency response and recovery plans — and provide training to all relevant personnel — to ensure consistency with protocols as defined by the National Response Plan and the National Incident Management System recently released by the Department of Homeland Security;

- Develop strategies to mitigate the redundancy of facilities and communications functions; and

- Conduct an inventory of all emergency response-related equipment to identify critical gaps.

The Department of Homeland Security defines response as the "activities necessary to address the immediate and short-term effects of an incident, which focuses primarily on the actions necessary to save lives, to protect property, and to meet basic human needs. Life-saving and life-protecting activities take precedence over other critical actions. Response activities include assessing preliminary damage and unmet needs; activating and deploying response resources into an affected area; providing access to and mobility within the area of operations; developing, coordinating, and executing an integrated incident management plan (which includes the activities of all response agencies); allocating existing resources in support of the plan and obtaining additional resources as required; and deactivation and standing down. It includes activities for providing basic life-support functions and services, triaging and treating personal injuries, minimizing damage to the environment and to property, both public and private, and planning for the transition from response to recovery within each functional area. Response operations also include law enforcement, investigative, and security activities conducted to address the criminal aspects of the incident."[7]

Through these same regional consortiums, the Commonwealth will enhance its capacity to respond to critical incidents by:

- Updating all agreements and response planning documents that support multi disciplinary response activities, including all Comprehensive Emergency Management Plan Annexes, regional plans, MOUs, incident command and management plans or directives and any guidelines affecting response;

- Identifying in the agreements the types and parameters of information exchanged, including standard methods of defining data, information, vulnerabilities and risks;

[7] *Department of Homeland Security, National Response Plan, page 9.*

- Establishing formal agreements or MOUs that identify the agencies, the points of contact and the parameters of exchanges of information;

- Ensuring that the process of exchanging information achieves collaboration among agencies and organizations; and

- Including in the exchange of information blueprints, schematics and other information on infrastructure on a need-to-know basis.

Goal #4 – The Commonwealth will improve the ability of first responders to communicate at the scene of a terrorist attack or other critical incident.

Local officials across the Commonwealth have complained for years that the ability of multiple public safety entities to effectively work together at the point of service – fires, accidents, natural disasters, search and rescues, etc. – has been seriously compromised because the radio systems used by independent entities operate on different radio frequencies. This means that first responders from one agency may not be able to use their radios to communicate with first responders from other agencies. This can result in a difficult – if not life threatening – operational environment, because every emergency response requires that information and instructions be communicated rapidly and accurately to all personnel that are on the scene.

There has been much debate about the best way to achieve this interoperability, particularly in light of confusion around the definition of "interoperability." For example, in the mind of some public safety officials, interoperability is something that is only necessary during a critical and/or catastrophic incident and can best be achieved through the deployment of temporary capabilities (stockpiled radios, command vehicles, etc.). Others believe that interoperability is a crucial part of day-to-day emergency and non-emergency service delivery. Under this model, the infrastructure that supports interoperability must be permanent and front line personnel must be trained so that these systems can be used daily. In many respects the challenge of providing equipment interoperability has less to do with technology and more to do with identifying and putting in place the processes, protocols and agreements necessary to support multiple agencies using an integrated system.

With the realization by the federal government that communications interoperability is indeed a crucial link in responding to emergencies (post-9/11/2001), federal funding has been made available to state and local agencies to assist in developing interoperability solutions. The Executive Office of Public Safety determined that a strategic plan was necessary to ensure that this funding was not only distributed to those agencies in need, but also that the resulting interoperability solutions are effective and promote interoperability among local, state, and federal agencies.

To this end, the Executive Office of Public Safety established an Interoperability Working Group, comprised of individuals with specific expertise in the area of communications, and who also represent the various constituent disciplines having a vested interest in this area. To facilitate the working group's efforts, a web-based survey instrument was developed to assist in evaluating the current state of interoperability among the Commonwealth's public safety and public service agencies. This survey provided much of the data upon which the development of a comprehensive interoperability strategy will be based. As a result of the

survey data and meetings with groups and individuals identified by the Commonwealth, an action and implementation plan and a realistic cost for achieving an increased level of interoperability was produced.

The EOPS interoperability survey was developed and available for input from July 16, 2003, through August 11, 2003[8]. One hundred and forty one surveys were completed, representing both public safety and public services agencies. Respondents, in many instances, represented multiple agencies in a specific field of public safety/service.

The majority of respondents to the survey (78%) indicated that the need for communications interoperability has increased considerably over the past five years. While interoperability is a priority of most agencies, respondents indicated that the most significant obstacles encountered in achieving a level of interoperability are limitations of funding (89.1%) and agencies operating on different frequency bands (73.3%).

To address these issues in a timely manner, the Interoperability Working Group agreed on two courses of action in developing the "blueprint" for interoperability in the Commonwealth:

- Currently available technology and equipment should be used where possible – improving existing networks and replacing those elements that may contribute to failure; and

- Ensuring connectivity and interoperability among existing regional systems throughout the Commonwealth

These elements will permit available funding to be used more effectively and provide interoperability among regional public safety and public service agencies, where it is needed most, in a timely manner. Accordingly, as a part of its SHSS, the Commonwealth will take steps to implement its statewide interoperability plan. Additionally, the Commonwealth will take steps to evaluate and upgrade (when necessary) the statewide wireless (voice and data) infrastructure that supports mission critical communications by federal, state, regional, local and private sector entities.

Goal #5 – The Commonwealth will improve its ability to recover from a terrorist attack or other critical incident.

The Department of Homeland Security defines recovery as "those actions necessary to restore the community back to normal and to bring the perpetrators of an intentional incident to justice. It entails the development, coordination and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual private-sector, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents. It may also include prosecution, incarceration, or other forms of punishment against perpetrators of intentional acts, as well as the seizure and forfeiture of their property."[9]

[8] *It should be noted that the survey was actually made available until October 16, 2003 for additional responses beyond the established deadline.*

[9] *Department of Homeland Security, National Response Plan, page 9.*

As a part of its SHSS, the Commonwealth of Massachusetts will take steps to provide for the rapid resumption of critical services and capabilities in the event that primary systems and capabilities are rendered non-functional. Specifically, the Commonwealth will:

- Merge independent assessments and asset inventories into a single, effective continuity of operations plan;
- Create a mechanism to link the continuity of operations plan with threat assessments and update the continuity of government plan;
- Link the continuity of operations plan with those of other relevant state and local entities; and
- Ensure that critical information and communication systems have adequate redundancy and disaster recovery capabilities.

State Prioritization Factors

- Threat, vulnerability and risk as established by a statewide TVR assessment process
- Level of regional collaboration
- Level of multi-disciplinary collaboration
- Population
- General Preparedness

COORDINATION

Upon taking office in January 2003, Massachusetts Governor Mitt Romney designated the Secretary of Public Safety, Edward A. Flynn, as the Commonwealth's Homeland Security Advisor (as defined by the Department of Homeland Security). Throughout 2003, Secretary Flynn and the Executive Office of Public safety took a number of steps to document the current status of the Commonwealth's Homeland Security efforts and to identify and document both gaps and priorities of state, regional, local and private sector entities involved in statewide homeland security activities.

EOPS conducted a statewide inventory of ongoing and planned homeland security efforts. This statewide assessment, completed in March 2003, included conducting a survey of 170 federal, state, local and private sector entities and completing a programmatic gap analysis and needs assessment.

Throughout 2003, the Executive Office of Public Safety convened and/or participated in hundreds of meetings across the state with law enforcement, fire service, emergency medical, emergency management, public health, regional and local officials as part of an aggressive outreach effort designed to solicit input from these entities to support the development of a statewide strategic plan.

As part of its effort to develop a statewide interoperability strategy, the Executive Office of Public Safety surveyed 150 public safety entities regarding operational, technological and other relevant issues associated with issues pertaining to the interoperability of radio system. As a part of this planning effort, a multi-disciplinary working group comprised of state and local officials was established to advise EOPS on the development of this plan. Additionally, a series of regional meetings were convened to solicit local input on interoperability and other related issues. The interoperability strategy will be completed and released in January 2004.

To support strategic planning and operational coordination, EOPS has established a Homeland Security Executive Committee comprised of senior officials from the Commonwealth's Department of Fire Services, Executive Office of Public Safety, Department of Public Health, Massachusetts State Police, Criminal History Systems Board, Massachusetts Bay Transit Authority (MBTA) Police Department, Massport, Executive Office of Transportation and Construction, The National Guard, Massachusetts Aeronautics Commission, and the Massachusetts Emergency Management Agency. Additionally, the metropolitan Boston Urban Area Security Initiative has appointed a representative to serve on the executive committee. The Homeland Security Executive Committee will work in partnership with local entities that will be organized into multi-disciplinary regional consortiums modeled on the Boston Urban Area Security Initiative.

Description of Jurisdiction:

The Commonwealth of Massachusetts consists of 351 cities and towns[10] and is approximately 8,257 square miles (of which 7,838 square miles is land area) with a population of 6,349,097. Its topography varies from shoreline on the eastern coast, interspersed relatively flat areas, and rolling hills, mountainous, and forested terrain, as one travels west. The majority of the population resides in the eastern third of the state and that area is predominately comprised of shoreline and a relatively flat topography.

[10] *It should be noted that while there are 14 identified counties within the Commonwealth, these counties do not possess any governmental oversight over individual cities and towns.*

Assessment of the Needs of Massachusetts Communities

Process Used to Complete the Jurisdiction Assessments

Officials from the Commonwealth attended a regional session in New York City where an overview of the ODP Assessment Process was explained by ODP and technical advisors from Texas A&M University's Engineering Extension Service (TEEX). After returning, meetings were held throughout the state in order to instruct local jurisdictions on completion of the 2003 Homeland Security Assessments. Additional meetings were held for State Agencies. These meetings were held to facilitate the completion of Jurisdiction assessments using the DHS/ODP's "Jurisdiction and Reference Handbook" for resource direction. Using these resources, workgroup members from each Jurisdiction participated in each session to ensure standardization in all assessments. Upon completion, the Massachusetts State Police (MSP) Criminal Intelligence Section (the entity charged with responsibility for completing the statewide threat vulnerability and risk assessment) reviewed and analyzed the assessments as a measure of quality control before the data was used by the Executive Office of Public Safety that is designated as the State Administrative Agency (SAA). The MSP reviewed assessments for completeness and ensured projections made were realistic for each jurisdiction based on planning factors for CBRNE scenarios. If an assessment required revision, the SAA released the information back to the jurisdiction to be revised and resubmitted.

Evaluation Plan for the State Strategy

The Secretary of the Executive Office of Public Safety (EOPS) has been designated by the Governor as the Commonwealth's Homeland Security Advisor (as defined by the Department of Homeland Security). As such, the Secretary will be the senior executive official responsible for overseeing and evaluating all activities related to the implementation of the SHSS. In support of this responsibility, EOPS will conduct a number of activities including the following.

- EOPS will work with its federal, state, regional, local, and private sector partners to establish, document, track, and evaluate specific milestones and performance metrics for each objective contained within the SHSS.

- EOPS will appoint a full-time employee from the Massachusetts Emergency Management Agency to serve as a liaison and point of contact for each regional consortium. This liaison will support and coordinate planning efforts on a regional basis, and track the activities of each specific region on an ongoing basis in accordance with the SHSS.

- EOPS will disburse to regional and local entities a portion of the 2004 funding upon the achievement of certain defined milestones (as identified in the implementation timeline; these milestones include the development of a risk based funding formula, completion of the statewide risk assessment, establishment of regional boundaries, establishment of regional consortium, etc..)

- EOPS will disburse the remaining 2004 funding to regional and local entities upon submission and approval by the Secretary of regional plans for implementing the SHSS, an equipment inventory by each region and a list of equipment to be acquired.

- EOPS will work with each region to develop a strategy to mitigate threats, vulnerabilities and risks identified through the baseline statewide risk assessment and ongoing risk identification activities. These mitigation strategies will include specific milestones and performance metrics that will be tracked and evaluated by EOPS on an ongoing basis.

- Each regional consortium will be required to provide a monthly report to EOPS on progress made in achieving identified implementation steps and milestones.

- Every two months, EOPS will convene a meeting of representatives from each region so as to receive updates on progress.

- EOPS will document progress made by each region in achieving objectives and milestones as defined by the SHSS (and subsequent planning and risk mitigation efforts) and how homeland security funding was utilized and the results of these activities.

- EOPS will, as required, submit reports to DHS regarding the implementation of the SHSS.

EOPS will conduct periodic meetings with its federal, state, regional, local and private sector partners to review the strategic goals, objectives, and implementation steps of the Massachusetts's State Homeland Security Strategy. Additionally, based on these periodic meetings, EOPS will have the responsibility for revising, as needed, the goals, objectives and priorities of the Commonwealth's homeland security efforts. EOPS will identify those revised goals and objectives through the standardized reporting format designated by the Office for Domestic Preparedness. This report will earmark those goals and objectives that have been revised and provide new supporting information regarding their measurements and assigned deadlines for completion.